LOPD EN LA EMPRESA

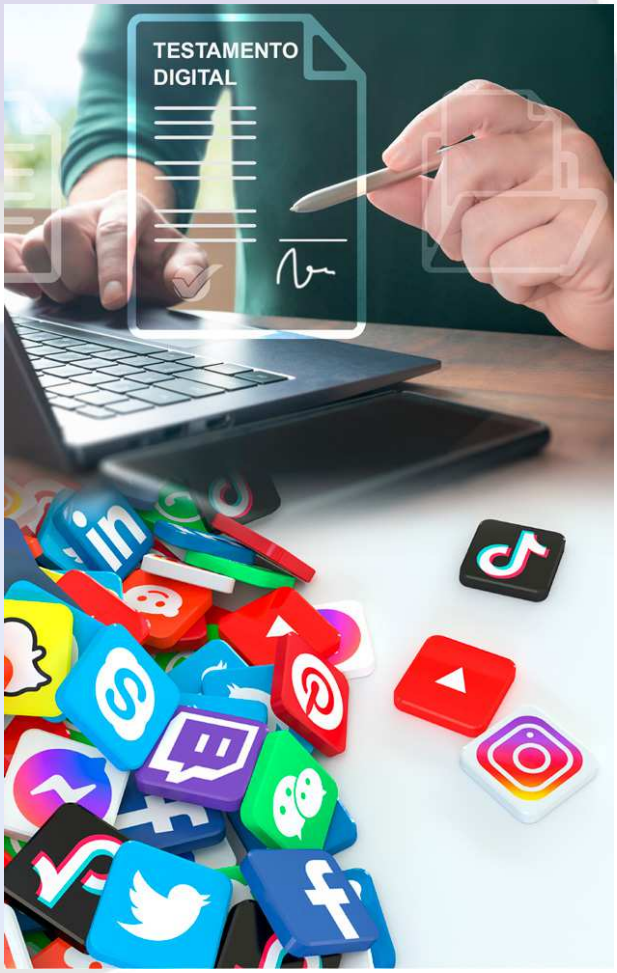
EL RGPD UE 2016/679 EN APLICACIÓN

Garantía de los derechos digitales: derecho al testamento digital (III)

En este boletín vamos a abordar uno de los derechos digitales contenidos en nuestra Ley Orgánica de protección de datos y garantía de derechos digitales (LOPGDD), el derecho al testamento digital.

¿Quiénes pueden solicitar ese derecho al testamento digital? En el artículo 96 de la LOPDGDD se regula el acceso a los contenidos digitales gestionados por los prestadores de servicios de la sociedad de la información sobre personas que han fallecido:

- Las personas que están vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos, se podrán dirigir a los prestadores de servicios de la sociedad de la información y solicitar el acceso a ese contenido e impartir instrucciones oportunas sobre utilización, destino o supresión. **En el caso de que el fallecido hubiese prohibido expresamente ese acceso, o bien una ley lo prohibiera, no se podría solicitar ese derecho de acceso.**
- El albacea testamentario y la persona o institución que se hubiese designado expresamente podrá solicitar el acceso con las instrucciones dadas por el fallecido en el mandato. También podrán solicitarlo de oficio, los representantes legales y en su caso el Ministerio Fiscal.



IMPORTANTE

El responsable del servicio al que se la comunique la solicitud de eliminación de un perfil deberá proceder sin dilación.

SANCIONES DE LA AEPD

Sancionada con15.000 € una entidad de selección de personal por no atender un derecho de acceso y supresión

En la resolución de la AEPD https:// https://www.aepd.es/es/documento/ps-00239-2022.pdf se sanciona a una entidad de selección de personal por no atender debidamente un derecho de acceso y supresión.

La reclamación fue interpuesta ante la autoridad alemana de protección de datos por una persona residente en Berlín, a la que le habían hecho llegar correos electrónicos con ofertas de trabajo sin solicitarlo. La AEPD es la que resuelve la reclamación, ya que la entidad sancionada tiene su establecimiento principal en España.

El reclamante manifiesta que la entidad de selección de personal le envío a su correo electrónico ofertas de empleo que él no había solicitado, por lo que ejerció su derecho de acceso y supresión de datos. **Ante esta petición, la entidad reclamada no contestó correctamente. Así se recoge en el apartado de hechos probados de la resolución.** El afectado solamente recibió por respuesta un correo en el que se le indicaba de forma genérica, con una escueta información, que los datos del afectado se habían obtenido de algún portal de empleo (*InfoJobs*, *Experteer*…) con los que la entidad trabaja y en los que estaría inscrito.

Además, ante el ejercicio del derecho de supresión, la entidad reclamada se limitó exclusivamente a eliminar su correo.

Se considera una infracción muy grave el impedimento, la obstaculización o la no atención reiterada del ejercicio de los derechos en materia de protección de datos.

IMPORTANTE

El responsable del tratamiento debe atender con diligencia las solicitudes de derechos en materia de protección de datos.

LA AEPD ACLARA

Internet de las cosas *(IoT):* Domótica. Internet de las Cosas: riesgos y recomendaciones (III)

En este boletín abordaremos el último capítulo dedicado al Internet de las cosas. En la página web de la AEPD se indican los riesgos y recomendaciones que debemos seguir con los dispositivos inteligentes con conectividad a Internet.

Los dispositivos *Lot* domóticos están evolucionando de forma constante orientados a ofrecernos servicios cada vez más confortables que se pueden controlar desde las Apps instaladas en nuestros móviles o bien, integrados en asistentes de voz. Así, por ejemplo, los sensores de temperatura y humedad, controladores de climatización y centralitas de alarma, entre otros.

Un dispositivo de *LoT* genera gran cantidad de datos que son tratados y enviados por distintos servicios en Internet. El riesgo es mayor cuánto es mayor el número de servicios que tratan estos datos personales. Así como, cuando utilizamos una App distinta en la que debemos registrarnos para cada fabricante.

Los dispositivos como mirillas digitales o cerraduras que se controlan desde la Apps implican el tratamiento de imágenes, video, audio e información sobre los hábitos de las personas, que podrían ser utilizadas para la generación de perfiles y diversas finalidades adicionales.

Las personas que adquieran este tipo de dispositivos deben adoptar una actitud crítica hacia las garantías de privacidad. Además, los fabricantes deben aplicar medidas de protección de datos por defecto y desde el diseño.

IMPORTANTE

El usuario/a de *IoT* debe cambiar las contraseñas predeterminadas de los dispositivos para evitar ataques de denegación de servicio *DDoS* y de acceso ilícito.

ACTUALIDAD LOPD

Cuando hay que revisar las medidas de protección de datos

Fuente: AEPD

El Reglamento General de Protección de Datos, RGPD, (art.24) y la Ley Orgánica 7/2021 (art. 27 que traspone el art.19 de la Directiva 680/2016) exigen que el responsable del tratamiento revise y actualice las medidas implantadas en el tratamiento para garantizar que cumple con la normativa de protección de datos. La propia norma establece que hay que llevar a cabo dicha revisión y actualización cuando resulte necesario.

Existen dudas entre algunos responsables sobre cuándo es necesario revisar dichas medidas, aunque, de forma implícita, esto ya está definido en la normativa de protección de datos citada en el párrafo anterior.

Dicha normativa exige que se han de aplicar medidas de forma selectiva. Es decir, la norma establece que hay que implementar medidas adecuadas para garantizar y poder demostrar el cumplimiento. Las medidas seleccionadas por el responsable han de ser las adecuadas y no simplemente una acumulación de medidas. La selección de medidas ha de ser un proceso racional basado en criterios de aptitud y eficacia de las medidas del tratamiento con el objetivo de garantizar y demostrar el cumplimiento de un tratamiento concreto.

Los artículos antes citados determinan cómo tiene que analizarse un tratamiento para determinar la selección de medidas que serán adecuadas. Por un lado, hay que tener en cuenta la naturaleza, el ámbito o la extensión del tratamiento, el contexto y sus fines. Por otro lado, hay que tener en cuenta los riesgos para los derechos y libertades de las personas físicas.

La naturaleza de un tratamiento determina el cómo está implementado: por ejemplo, automático, manual, mixto, en qué operaciones se estructura el tratamiento, si se ejecuta en la nube, en el móvil, si incluye operaciones biométricas y decisiones automatizadas, si participan encargados de tratamiento, si se llevan a cabo transferencias internacionales, etc. (…)

La normativa de protección de datos no exige que dicha revisión sea periódica, pero implícitamente exige que se esté al tanto de los cambios en la naturaleza, contexto, ámbito, fines y riesgos del tratamiento para actuar en consecuencia.

Puede ver más información en el siguiente enlace

Cuando hay que revisar las medidas de protección de datos

EL PROFESIONAL RESPONDE

¿Cómo puedo proteger la información de mi empresa? (I)

Las empresas se enfrentan hoy en día a múltiples riesgos que pueden poner en peligro la información de la empresa. Lo primero que tenemos que realizar es una selección de la información que queremos proteger en base a que, si se accediese a ella de forma ilícita o se alterase, paralizaría nuestra actividad, con las pérdidas económicas que ello conlleva.

La clasificación de la información se puede establecer en varias categorías:

- **Confidencial**: es una información muy sensible para la empresa, incluida aquella que contenga datos de carácter personal de categorías especiales, a la que solo puede tener acceso la Dirección y el personal autorizado para el desarrollo de sus funciones. Deberíamos implementar los controles necesarios para limitar ese acceso.
- **Interna**: se trata de aquella información que es accesible a todo el personal y que todos deberían de conocer, por ejemplo, las políticas de seguridad y de protección de datos de la entidad. Esta información no debería difundirse a terceros, a menos que exista una autorización de la persona responsable de garantizar la seguridad de la información.
- **Pública**: es una información que la empresa ha hecho pública, por ejemplo, a través de su página web corporativa o bien, en catálogos dirigidos a los clientes. Este tipo de información no requiere de control especial.

IMPORTANTE

Después de realizar la clasificación de la información es necesario valorar su criticidad y determinar su riesgo para aplicar las medidas técnicas y organizativas.

• AUTOR: JULIO CÉSAR MIGUEL PÉREZ